Microsoft Ignite
November 18-22, 2024
Session: GS06
Speakers: Aidan Marcuss, Bob Lord, Dave Dame, David Weston, Jack Cable, Mark Lambourne, Navjot Virk, Paul Gravestock, Pavan Davaluri, Sandra Lee

[MUSIC]

Speaker 1: Please welcome Pavan Davaluri.

[APPLAUSE]

Pavan Davaluri: Thank you. Good afternoon. It's great to be at Ignite here with all of you and folks online. Collectively, you represent hundreds of millions of employees across a diverse set of business from almost every corner of the globe who have chosen to win with Windows. For that, I'm incredibly grateful. The energy at Ignite is real. It comes from the opportunity to transform productivity in the era of AI. Taking advantage of that energy and that opportunity takes real work. Work from people in this room to move your organizations forward, to deliver on the fundamentals of security and reliability while seizing the opportunity to empower your employees and to build a real path forward to move off of aging technologies like Windows 10 while delivering measurable return on that investment and show progress. These challenges and opportunities are both complex and motivating, and why we're building the next generation of Windows for your businesses for today and for tomorrow. At the end of our time together, I hope you'll see for yourself three things. First, that Windows is the most reliable and secure platform on earth. Second, modernizing your endpoints with Windows 11 delivers real business value. And third, with AI woven across Windows you can unlock new levels of productivity for your employees. Let's start with job number one, keeping your organization reliable and secure. Windows has always been the platform for the world's innovation by creating an open operating system for the best product makers to do their work. Windows has been able to meet the needs of over a billion customers worldwide and, as a result, Windows has become a part of the global infrastructure. With that comes an incredible responsibility to remain committed to each of you, delivering you the most reliable, most secure platform on earth. The incident that impacted 8.5 million devices in July was a stark reminder that we must remain vigilant and continue to innovate on a platform that you can earn trust. In response, we're announcing the Windows Resiliency Initiative to firm

our commitment to making Windows reliable and secure for all our customers, including mission-critical workloads.(Onscreen text: aka.ms/WinWithSecurity) As a part of this initiative, we're working together across the industry and will improve reliability based on lessons from July with new changes in standards in the OS, protect against malware and script attacks with stronger controls for apps and drivers, prevent phishing attacks by enhancing identity protection and find a new balance to empower employees without the need for local admin privileges. Taken together, this will ensure that Windows remains the most reliable platform on earth. Please welcome David Weston to the stage to share more about the Windows Resiliency Initiative. David? Alright, let's do this.

David Weston: Alright. Awesome, thank you, Pavan. After the July incident I talked with hundreds of customers, including CISOs, CIOs and incident responders, including many of you here today. They told me about the costs, challenges and pain points you experienced with the incident and the associated recovery, and you told us that you want to keep your existing security capabilities while at the same time making it easier to prevent and recover from issues. Your feedback provides essential learning we're applying to ensure incidents like this never happen again. You told us we need to act on three big things. One, making Windows easier to recover. Two, strengthening the resilience of critical security tools and drivers and three, improving the overall security of the platform so it's more effective and self-defending, reducing the overall complexity. We heard you and we are acting. I'm here today to tell you what we're doing to address all of this feedback, so let's get started with the first pillar of the Windows Resiliency Initiative, improving Windows reliability. We are working on new Windows capabilities to enable security product developers to build their products outside of kernel mode. We call this our Windows Resilient Security Platform. This is a flexible security API set and data collection points that can be used to build endpoint security products like detection and response or antivirus outside of the kernel. This means security products like antivirus or EDR solutions can run in user mode just like an app does. We're assuring this platform will enable security solution providers to have the access they need to detect and respond to threats without introducing complexity into the kernel. This change will help end user protection and antivirus products provide a high level of security and easier recovery and, most importantly, there'll be less impact to Windows in the even of a crash or a mistake. We plan to have a private preview to share with our security product ecosystem in July of 2025. Next, we heard you on the need to recover Windows quickly during an incident and we built something to do this at planetary scale. Coming to the Windows Insider Program in Q1 of 2025 and then the broader Windows release after that, we are building a new solution for Quick Machine Recovery.

[APPLAUSE]

Quick Machine Recovery can execute targeted fixes from Windows update on machines, even when Windows is unable to boot. With this new solution, we can use the trusted Windows pipeline to quickly deploy fixes that address files, drivers or any other operation needed to recover a non-bootable machine. In addition to recovery capabilities built in to Windows, we want to make sure the security products you have today are more reliable and more resilient, so we included the entire Windows ecosystem in this initiative. To accomplish this, we brought together our industry-leading security partners along with the US Cybersecurity and Infrastructure Security Agency for a Windows endpoint security ecosystem summit.

(Onscreen text: aka.ms/WinSecuritySummit)

The goal was to define new ways to increase resilience across the ecosystem and ensure Windows remains an open platform, enabling user choice and innovation while also maintaining the highest standards for security. Microsoft Virus Initiative partners from around the globe, including Microsoft Defender, are committing to taking specific steps to enhance both security and resiliency. One of the most important steps is adopting safe deployment practices, which means that all security products updates must be gradual, they must leverage deployment rings and must employ monitoring to ensure any negative impact from an update is kept to an absolute minimum. Partners must also conduct additional security and compatibility testing for components like a security kernel driver to ensure issues are detected before any incident can occur. Microsoft and our MVI partners are also working together to develop strengthened incident response processes for streamlined coordination to move quickly and decisively together to keep everyone up and running. As I mentioned earlier, CISA is an important participant in determining a new set of security and resiliency standards for Windows endpoints. They are providing a framework for the whole IT industry to ensure that all partners, customers and organizations are able to stay ahead of evolving security threats. CISA recently released guidelines for how the IT ecosystem in the United States must use safe deployment practices to avoid widespread issues that impacted so many organizations and customers in July. Now, let's here directly from CISA.

Bob Lord: Hey, everybody. Thanks so much for having us. My name is Bob Lord and I'm a Senior Technical Advisor at CISA.

Jack Cable: My name is Jack Cable and I'm a Senior Technical Advisor at CISA, the Cybersecurity and Infrastructure Security Agency. CISA leads the nation's efforts to manage and reduce risks to our critical infrastructure and federal civilian government systems.

Bob Lord: We were pleased to participate in the Microsoft Windows endpoint security summit and look forward to ongoing collaboration for ways that we can all work together to make sure that we are building software that is safe, secure and resilient. To that end, CISA has published a white paper on safe software deployments, and in it we talk about some of the major elements of producing software that is not just secure by design, not just secure by default but is secure through the delivery to the customers, whether that's software that you deliver directly or through online services.

Jack Cable: This paper aims to fill existing gaps in the literature by providing a foundation for six common steps of software deployment. It's our hope that through this guidance software manufacturers can understand how to deliver updates to their customers in a manner that is secure and reliable such as through internal testing and canary releases.

Bob Lord: Thank you for your attention. We really want to have a larger conversation about what it takes for the industry to deliver software that is safe and secure and resilient. Thank you.

David Weston: In addition to the work we are doing with CISA as part of Microsoft's Secure Future Initiative, we are heavily investing in safe languages to enhance the safety of our code. This commitment also aligns with CISA's secure by design pledge. We're applying this new approach to our security platform and other key areas like Microsoft Surface's firmware and the Pluton security processor firmware. Part of becoming resilient is also increasing the prevention of attacks, so more security has been built into the operating system and not bolted on later. This reduces complexity and ensures you deploy less software that could become the next failure point. This is why we are targeting the most critical elements of Windows 11. We analyzed the trillions of security events we get every day from over a billion endpoints and combined that with the information we get through AI and the Microsoft Threat Intelligence Center. Based on this, the largest source of attacks are clear. Unverified application, credential-based attacks and admin privileges. Let me tell you how we're addressing this to keep you safer. First, we are asserting stronger controls for what app and drivers are allowed to run in the Windows OS. This is important as unverified apps and drivers lead to malware and script-based attacks, and most malware and ransomware apps are unsigned, which means they can be authored and distributed without being provably safe. Smart App Control and App Control for Business policies provide peace of mind that only verified apps can run on your device. This has always been possible with products like App Control or AppLocker, but they could be really complicated to manage, but with the power of AI we've made it much simpler to deploy. IT admins can simply select the Microsoft Cloud Policy in the App Control wizard, which enables millions of known safe apps to run regardless of where they are deployed from, and line

of business apps unknown to Microsoft can be easily added through policy changes or via Intune managed app deployment. Robust app control ensures that only verified apps can run, and this eliminates attacks like malicious attachments or social-engineered malware. Now let's talk about how we're stopping identity attacks. We all know phishing is a huge problem. Microsoft Entra data shows that more than 600 million identity attacks occur per day, and over 99% of those are password-based. In response, we've hardened Windows Hello, which is our Windows built-in MFA solution. We're using the new hardware included in Copilot+ and secured-core PCs to isolate and protect the biometrics involved as well as to protect credentials, and Windows Hello has been extended to support passkeys, which means much of the web can be protected with MFA seamlessly. Now, you no longer need to choose between a simple sign-in and a safe one. Windows Hello is also being used to protect things like Windows Recall and personal data encryption. Finally, the new feature I am most excited about creates a new balance to empower employees without the need for local admin privileges. Over-privileged users and applications are a long-standing challenge and they create significant risk. In fact, compromise of high-privilege users and apps make up the bulk of attack vectors used in breaches. Our Microsoft Digital Defense Report calls that out. 93% of our ransomware incident response engagements revealed insufficient controls on privileges as well as lateral movement, so we're introducing administrator protection. With admin protection employees have standard user permissions by default so they can still make Windows systems changes, including app installation, but only when necessary and only after authorizing the change using Windows Hello. Admin protection will be incredibly disruptive to attackers as they no longer have elevated privileges by default, and it will help ensure that employees, not malware, remain in control of Windows. I am incredibly excited for you to try these new features and share your feedback. Rest assured, Windows remains committed to staying an open platform for innovation, providing flexibility and customer choice without locking down the operating system or determining a single way of working while enhancing security and reliability for all. That's what the Windows Resiliency Initiative is all about. Moving to Windows 11 is a key part of achieving an optimal security posture because the latest OS is always the safest OS. Windows 11 is the most secure operating system we have ever built because we applied a secure by design strategy from the very first line of code. Now, let's talk about what sets Windows 11 apart. First, we have established a hardware security baseline. This ensures every Win11 PC has consistent hardware security forming a secure foundation, and this foundation gives you confidence in the security of the operating system and all other experiences built on top of it. Windows 11 is more secure by default. We are adding new security capabilities with each release to stay ahead of emerging threats. These changes include enabling credential protection by default, removing legacy attack surfaces and moving

old code out of the kernel. We have confidence that our Windows security strategy is raising the bar for your protection. After transitioning from Windows 10 to Windows 11, research shows a 62% drop in security incidents, three time reported reduction in firmware attacks and 80% of customers are telling us that new Windows 11 PCs provide better security and data protection than their older devices. As I said earlier, the latest version of Windows is always the most secure version of Windows and it's only getting better. For example, we just added personal data encryption to Windows Enterprise. This is a second method of encryption on top of BitLocker to protect your most sensitive files. These files can only be decrypted by a user via Windows Hello. We've also added things like additional kernel protection with hardware, more safe language usage across the operating system and we've even introduced a new, hardened printer stack. Our security teams are working hard for you so you don't need to spend your time enabling security on new or upgraded PCs, and we will continue to innovate based on your feedback across client and cloud. The most important action you can take today to secure your organization is to move to Windows 11 on a new, secured-core PC, or with Windows 365 cloud PCs, because Windows 11 is designed to meet both today and tomorrow's threats, not those of 10 years ago. Security is a team sport, so everyone needs to adopt the security and reliability practices outlined in the Windows Resiliency Initiative. Please keep your feedback coming. We are listening and we are acting so you can count on Windows for everything you do.

[APPLAUSE]

Mark Lambourne: We play a critical role in supporting and enabling global economies. The London Stock Exchange Group is one of the world's leading financial market infrastructure providers.

Sandra Lee: Windows 365 and the Windows 11 provided us with the capability, the operational resilience, the security that we needed to be able to provide a secure platform on which to build our products and services off.

Mark Lambourne: By having one platform, engineering effort for us has shrunk down to about half. Under our previous set of capabilities, developers had to log on to multiple different desktops.

Paul Gravestock: We feel the future is very exciting with the capabilities that these tools give us to be able to rapidly deploy and deliver products to our clients.

Sandra Lee: Using the Windows 365 platform, our developers are able to access GitHub Copilot to be able to leverage from the AI capability to more efficiently develop their code.

Mark Lambourne: On new platform Windows 11 devices and Windows 365 gives us that strong foundation, well-designed, well-architected to bring new innovation with much lower friction, much lower time to market and get business value delivered more quickly.

Sandra Lee: We've seen an increase in customer satisfaction but also, more importantly, from an operational perspective, the reduced time and effort to maintain and sustain a standard secure operating platform.

Mark Lambourne: We're really excited to see the value that it brings. We think it might be quite profound for our organization.

[MUSIC]

Pavan Davaluri: That was awesome. Windows represents an opportunity to modernize your endpoints, both for your PC fleet and your cloud clients. Just like the London Stock Exchange, you too can create a strong foundation to deliver innovation and business value faster. Today we'll talk about the benefits of Windows 11 and how we're enabling the move from Windows 10 for your PCs, VDI and DaaS solutions. Customers are choosing to modernize their fleet for three key reasons. First, better security and resiliency. Second, streamlined management and compatibility, and third, increased employee productivity. Together, these benefits will deliver meaningful return on investment for your business. Let's start with your PC fleet. With Windows 10 end of support coming October 2025, now is the time to move to Windows 11 with confidence. We understand change isn't easy, and we're working hard to make the move to Windows 11 more compelling and easier than ever.

(Onscreen text: aka.ms/Win10EOS)

As you just heard from David, Windows 11 is more secure by default and by design. It's the single most important reason customers are moving to Windows 11 today. Customers like Carlsberg are taking advantage of Windows 11 security baseline to protect their entire global workforce. They have peace of mind knowing their endpoints are hardened with the latest security features designed to protect against modern and evolving threats. We've simplified managing the move to Windows 11 to minimize disruption to your workforce. Windows 11 can be managed with the same tools and processes you use with Windows 10 today, and Windows 11 is compatible with all of your apps, backed by our App Assure promise. Once you've transitioned, it's easy to stay up to date. Regular Windows 11 updates are 40% smaller in size. That's why iconic companies like Levi's are leaning into the future and making the move. After piloting Windows 11, Levi's realized the benefits of a streamlined and productive employee experience. They quickly deployed Windows 11 to their global workforce, utilizing Autopilot to ship new devices directly from the factory to employees, who securely set up

their new PCs with Intune and Entra ID. Windows 11 is faster and more productive for employees. You can choose the right modern hardware for your organization from Surface and from our incredible Windows ecosystem partners. Newer Windows 11 devices deliver vastly improved performance, even from just a few years ago. When you compare these older Win10 devices that don't meet the Windows 11 hardware specifications, the difference is clear. Employees get over double the battery life and more than three times the faster performance. Upgrading from an older Windows 10 PC to a new Windows 11 PC will significantly boost productivity of your employees, and this year we've raised the bar on what you can achieve with new PCs built for AI. In May, together with our silicon and OEM partners, we announced a new category of devices, Copilot+ PCs. They're built for productivity and they're the fastest, most intelligent and secure PCs available. Top Copilot+ PCs are up to 58% faster than a MacBook Air M3, and all the benefits of security, manageability and increased productivity come together this week with two announcements we're sharing. I'm excited to announce Windows Backup for Entra ID, available in public preview this spring. You've told us that personalizing a new PC is time-consuming for employees.

(Onscreen text: aka.ms/WinWithWindows)

With Windows Backup, you can easily transition new PC settings and preferences and set up a new PC or perform a traditional reinstall. Preferences like desktop background and icon size appear on the new PC in the same way that they did on the old device. This reduces the time spent on set-up so employees can be productive faster, while significantly reducing IT overhead and help desk calls. I'm also thrilled to announce Windows Hotpatch, coming to Windows 11 Enterprise and Windows 365 this spring.

[APPLAUSE]

It's one of my favorites.

Pavan Davaluri: Using Windows Hotpatch through your autopatch settings in Intune, you can now seamlessly deliver Patch Tuesday security updates directly to your employees on day one. With Windows Hotpatch, 65% of Patch Tuesday security updates are directly delivered without requiring a restart. Reducing restarts and interruptions means security updates get deployed 60% faster. Over a million businesses have already made the move to Windows 11. These companies are seeing faster workflows and increased productivity and cost savings from fewer help desk tickets and reduced security instance. In fact, according to Forrester research, moving to Windows 11 delivers an amazing 250% return on investment over three

years. Modernizing isn't just about cost savings. It's about our collective responsibility and impact on the global economy and the environment.

(Onscreen text: Microsoft.com/Sustainability)

Like you, Microsoft has committed to advancing sustainability and adopting Windows 11 helps in achieving your company's sustainability goals. Windows 11 reduces energy use as the world's first carbon-aware OS and offers Energy Saver, increasing energy efficiency by up to 22%. More devices are manufactured using recycled materials and more renewable energy. For example, Surface enclosures use 100% recycled aluminum alloy and 100% recycled rare earth materials. Programs are available to reduce e-waste with the recycling and refurbishment opportunities available across our ecosystem partners. There's also the option to extend the life of older hardware with Windows 365 without sacrificing security protection or experience. Together, we can make a difference in sustainability as we move to the next generation of Windows. For those of you who've already moved your PC fleet to Windows 11, thank you. For those of you that are working towards the October 2025 deadline, we look forward to partnering with you. We want all of you to experience the benefits of better security, improved management and increased productivity that Windows 11 delivers, and all these benefits extend to the cloud. Three years ago, we launched Windows 365 in response to customer demand for a simple, secure SaaS solution for Windows to empower people to work flexibly from anywhere, and we named this new category of end user computing Cloud PC. It fundamentally re-imagines VDI and DaaS by lowering cost, delivering the best-in-class employee experience and helping IT be more efficient. Windows 365 securely streams your full personal desktop with all your apps, content and settings directly from the Microsoft Cloud to any device. It's simple to deploy with just a few clicks in Intune and scalable to thousands of PCs. Windows 365 gives you the flexibility to have a tailor-made Windows experience for every employee in every organization. To tell you more, please welcome Aidan Marcuss to the stage.

[APPLAUSE]

Pavan Davaluri: Alright, Aidan. Let's do this.

Aidan Marcuss: Alright. Thank you, Pavan. It's great to be here today with all of you. Customers choose Windows 365 because they can deploy in hours, not months, connect in seconds, not minutes, all while reducing their IT infrastructure and management complexity. Customers like Johnson & Johnson deployed Windows 365 to modernize the way they manage their desktops, to improve the user experience, lower cost and complexity and simplify their operational environment. Wells Fargo is moving off of legacy

on-prem VDI to Windows 365 as part of a wholesale modernization strategy. Based on user personas, they're bringing multiple workloads to the cloud for better security, better efficiency and lower TCO. Your energy, engagement and feedback powers our team to keep innovating. Thank you. You can hear directly from Johnson & Johnson and Wells Fargo tomorrow in one of our breakout sessions. They are among thousands of customers who are adopting Windows 365 to serve a wide variety of scenarios within their organizations, and with the ability to pick exactly what you need with options from basic productivity to developer machines to powerful GPU machines capable of handling the most sophisticated, high-capacity computing tasks, it's not just the best way to modernize your on-prem VDI. It gives you way more flexibility to do more with Windows 11. Windows 365 now is going where you said you needed it, on any endpoint for everyone in your organization. It's great on Windows 11 PCs, including new Copilot+ PCs with unique features like boot directly to your Cloud PC and switch to your side-by-side cloud desktop. In fact, Windows PCs are the number one endpoint for Windows 365, but with broader Windows app support, new solutions like Frontline Shared, new cloud-first endpoints and even mixed reality, Windows 365 is built for you and how you need to use it. Let's go deeper into the new solutions we announced this week, starting with the Windows App. Launched earlier this year, it makes Windows 365 available for every employee however they want to work. The Windows App allows you to access Microsoft's virtualization services on an iPad, a Mac or a Windows PC with a single click. It's simple to use, consistent across endpoints and delivers a complete Windows solution. Hundreds of thousands of you have embraced it and are starting to use it. Now we're expanding the Windows app to even more endpoints, bringing that Windows app to the Android platform. It's in preview today and available in the Google Play Store.

(Onscreen text: aka.ms/WinWithW365)

I can't wait for all of you to try it. Based on your feedback, we're going to enhance the way you can manage the Windows App. Windows 365 is a popular choice for temporary and mobile workers as well as bring-your-own-device scenarios, and we want to make it even easier and more secure for you. We're excited to announce mobile application management support in the Windows App. Mobile application management enables lightweight but still highly secure management to support employees and contractors who need to access data in applications on their personal devices. Only Windows 365 can enable secure, managed access everywhere. This week, we also announced a new solution for Frontline workers. Windows 365 Frontline Shared delivers the same secure, high-fidelity Windows 365 experience but takes a single Cloud PC and lets it be shared across many Frontline workers during the day. This is something you asked for on behalf of your employees

who need to use Windows 365 occasionally to do their job. With Frontline Shared, every person gets the same, consistent apps and set-up every time they log in. Our team prioritized getting this out because you told us you want to extend Windows 365 to more employees so they can do their best work on Windows. Here at Ignite, we also announced our first dedicated device for Windows in the cloud, Windows 365 Link.

(Onscreen text: aka.ms/Windows365Link)

This new hardware expands the Cloud PC category by connecting you directly to your productivity in the cloud. You asked for a simple, secure endpoint with no data or information left onto the device, and Windows 365 Link delivers just that. It's admin-less, it's password-less and configured with strong security defaults that cannot be disabled. It's the perfect device for employee working at a hotdesk, a call center or another shared or specialized space. It sets up in literally minutes with two 4K monitors as well as all kinds of common peripherals. It's got a full complement of ports and Bluetooth. You can pick the identity access choice that's right for you, including biometric keys and multi-factor authentication using Entra ID. Windows 365 Link helps you lower your total cost of ownership without sacrificing employee experience or requiring new tools or learning new processes. Let's take a look at just how easy it is to get started with the Windows 365 Link. I want you to watch this clock, which is in the corner, as we get set up. The device has arrived and Alex, our IT admin, is ready to begin setting up a shared hotdesk in the office. He gets it connected to all the peripherals needed. He plugs in two monitors, the USB dongle to connect the wireless mouse and keyboard, the Ethernet cable and the camera. All set up, he powers the device on. Now the simple set-up process begins. The Link is Wi-Fi, but because Alex plugged in an Ethernet cable that step is just skipped. All he has to do is sign in with his Entra ID, which will connect the device to the corporate tenant. Alex enters his work email address and authenticates using a security key with a PIN. The device is now automatically joining the company's Entra tenant and enrolling in Intune, enabling the device to be cloud-only and fully managed. Entra's strong authentication methods, conditional access policies and single sign-on eliminate the need for a password on this endpoint, and security features like Secure Boot, BitLocker and Hypervisor-protected code integrity are enabled by default and cannot be disabled. There's no local data, no local apps, so corporate data is never on the device. With no local admin user and strict application control policies, no local software can be installed. The set-up process is now complete, seamlessly connecting Alex to his personal Cloud PC right where he left off, all done in under three minutes. This device is now ready for any Windows 365 user in that tenant. Now Jaylene, an employee, sits down at the desk to begin her day. She plugs in her FIDO2 security key to the device, touches the biometric reader to authenticate and

connects to her personal Cloud PC. The presentation she's been working on is opened up right where she left it. She makes progress, she does some work and then signs out of the device. With the desk open, employees come and go throughout the day, each quickly getting their Cloud PC. Less than three minutes from box to productive with the Link. The simple, secure, purpose-built device for Windows 365.

[APPLAUSE]

Now this is the first dedicated device for Windows 365, but we're not stopping here. Cloud PCs are designed to complement your Windows 11 end user computing estate. To do that, we'll enable more endpoints and form factors, scaling with our OEM ecosystem partners to unlock more value and more options for you. Now, let's talk about how great Windows 365 is on a Windows 11 PC. Here, Serena, a designer, is using her Copilot+ PC to log in to her GPU-powered Cloud PC, access a super-powerful CAD application with Creo and then join a Teams call and share that design with a colleague. What she's doing in that scenario, she's actually mixing the power of her Copilot+ PC where she gets all the Teams effects, the framing, the audio quality, with this powerful GPU in the cloud, seamlessly blending those to get done the work that she needed to get done and share it. Windows 365 extends the Windows experience everywhere you work with the performance and security you can count on. It's really easy to get started with Windows in the cloud today. We have some breakout sessions tomorrow, please join us for those where we'll go into depth into all of these things. Now I'll hand it back to Pavan. Thank you.

[APPLAUSE]

Pavan Davaluri: That is amazing, Aidan. Thank you, thank you. The work you're doing to secure and modernize with Windows 11 today will be the foundation of employee empowerment tomorrow. Windows has from its very inception been about enabling each of us to do our best work, and that truth remains at the heart of why many of you choose Windows, so we will continue working to empower your employees, making Windows the most productive platform on Earth. Today, most employees and enterprise have both Windows and Microsoft 365, and we can improve their daily experience by innovating on how Microsoft 365 and Windows work together. Simple changes make a big difference, like making it easier to find your M365 apps and content directly from File Explorer with access to modern file types like LUP and the ability to connect directly with collaborators using the people card, M365 companions and such. We will also introduce a new set of experiences that puts your Microsoft 365 people, files and calendar right on your taskbar. This makes it easier to find people in your org and collaborate with those you work with the most, giving you instant access and ability to

share the most important content and helping you manage your time. All this just a click away on your Windows desktop. These are meaningful steps forward for your employee's productivity, and AI gives us an opportunity to make a giant leap forward. This is why we're building Windows to be the destination for AI. Copilot+ PCs set a new bar for how a PC can enable productivity. They're the most secure, most intelligent PCs we've ever built and they deliver new standards in performance, reliability and quality, but most importantly, they are the first PCs built for integrated, concurrent, pervasive AI workloads. With co-engineered silicon from AMD, Intel and Qualcomm, they deliver the world's most advanced AI inferencing capabilities directly on a laptop. Copilot+ PCs combined with Windows and the Windows Copilot Runtime are built from the ground up to extend Microsoft's Copilot stack to the client.

(Onscreen text: aka.ms/WindowsCopilotRuntime)

They will enable innovations, enable the world, quite frankly, to bring their best innovations to Windows, from Anthropic, Meta, OpenAI, Hugging Face to ISVs like Adobe, LiquidText, Microsoft 365 and countless more who are already taking advantage of the platform, all with the simple objective of not just solving challenges of today, but helping you leap forward and harness AI for tomorrow. I'd like to introduce Navjot Virk to tell you more, but before I do that, let's take a look at how Copilot+ PCs and Windows will empower your employees.

[MUSIC] [APPLAUSE]

Navjot Virk: Thank you, Pavan, and I hope all of you are as energized by this video as I am. There's a lot to cover, so let's dive in. Empowering employee productivity is at the heart of everything we build. By leveraging the world's most powerful AI, we're creating new experiences for your employees, helping them be more productive, collaborative and satisfied at work. This is designing for business AI. Our innovation is centered on three important aspects of employee productivity. First, helping you find the information you need fast. Second, simplifying your workflows by making it easier to get things done. Third, enabling you to more effectively collaborate so you can be seen, heard and understood. As a result, we have created an experience with less friction, richer context and greater capabilities for everyone. We've heard from you and your employees loud and clear that one of the most frustrating problems you face every day is finding what you're looking for on your PC. Hold on, my mic is trying to misbehave. Okay. Today, there are billions of searches on Windows and way too many of them don't come back with the results you're looking for, wasting valuable time. With Copilot+ PCs and their powerful NPUs, we are making finding what you're looking for a whole lot easier and smarter. We are making Windows Search intelligent by unlocking

natural language search. Just describe what you're trying to find, whether it's text or images, and Windows will search based on your intent, even if it doesn't match the exact file name. Search for last month's sales report, an important contract or strategy document by simply describing what you remember. Next year, we will bring Federated Intelligent Windows Search for Microsoft 365 customers, so you can easily find not only your local files but also your OneDrive for Business files. We'll be bringing Intelligent Windows Search to settings and expanding to the Windows search box next year too. With Recall, we introduced an entirely new way to securely search for things you've seen on your PC. We appreciate all your early feedback and want to recognize the contribution of researchers and the security community in shaping Recall. For managed devices, in managed organizations, Recall comes with granular management controls and is off by default. We've also added meaningful security enhancements, including additional layers of data protection and Windows Hello protection. As a result, this experience is one of the most secure designs we have ever built, raising the bar for personal data protection, so you can have peace of mind when you decide to enable this feature for your employees. Of course, we're not done. We'll continue to work with all of you on building manageability, trust and value for new AI experiences like Recall on Windows. With tools like Federated Intelligent Windows Search and Recall, we're helping your employees easily find what they're looking for in a way only Microsoft can. Your employees also tell us it's easy to get distracted and pulled away from what's important when you're switching between tasks and navigating between applications. That's why we're bringing AI when and where you need it to simplify your workflows. Microsoft 365 Copilot is your AI companion for work. Copilot is already becoming a daily habit for people around the world. Nearly 70% of Fortune 500 companies are using it for tasks like summarized text, drafting responses and catching up on what they might have missed. We are accelerating our ambition to give every employee a Copilot and to transform every business process with agents build in Copilot Studio. With the Copilot Key on Copilot+ PCs, all that incredible innovation is just a click away, making it faster to access Copilot whenever you need it. Now, by leveraging the power of MPU to run AI models locally, Copilot+ PCs help you get even more value from your Microsoft 365 Copilot license. We're announcing local rewrite and summarize in Outlook and local rewrite in Word so you can get real-time and private AI inline. This experience is Cyber Executive Order-compliant, unlocking AI in even the most regulated industries. Now, let's talk about one of my favorite features, Click to Do. With Click to Do, we are introducing an all-new powerful productivity paradigm that puts AI right at your fingertips to assist with common tasks across all your applications. Click to Do connects you to AI actions based on the context of what's on your screen, making it faster and easier to get things done. Just press the Windows Key and left click, or invoke from one of our most-loved apps, snipping tool, and let AI analyze your

screen. It automatically shows you the most relevant set of AI actions based on what you've selected. You can get access to AI writing tools like rewrite and summarize directly in line, or get recommendations for other helpful visual tools to quickly complete your task. Click to Do works with all of your line of business applications. For example, you can do things like summarize a knowledge-based article you're reading in ServiceNow. Content on your screen is never saved so your information stays secure and private. Click to Do saves you time and keeps you focused. Windows wants to help everyone do their best work. Narrator is a screenwriting application built in to Windows, designed to help people with no or low vision understand and navigate what's on the screen. Now that experience is even better. With the power of NPU, AI generates a richer description of visual content like graphs, charts and images so your employees will get more equitable access to information with richer descriptions. Whether it's Copilot at your fingertips or Click to Do with AI actions when and where you need them, Copilot+ PCs empower every employee to simplify their workflow. Finally, we have built Copilot+ PCs to be the best PCs for employee collaboration so everyone can be better seen, heard and understood in meetings. We are introducing super resolution in Teams. Leveraging the power of the NPU, Teams automatically enhances incoming video quality when collaborators have bandwidth constraints or a poor network connection. Coupled with battery life and performance enhancements, Copilot+ PCs are the best endpoint for Teams. Live captions with live translations turn any audio into a single, consistent English-captioned experience in real time on your screen. With translation support for over 40 languages into English, we're making it easier to collaborate with fewer language barriers. Windows Studio Effects provide helpful visual and audio filters so you can look and sound your best, whether you're on Teams, Zoom, WhatsApp or any other video conferencing app. These experiences matter. With simpler workflows, ability to find information faster and tools to be better collaborators, your employees will feel more empowered and productive when working on Windows. We invite you to come and see us on the show floor where you can learn even more. The NPU-powered experiences I've shown you, including the ones in your Microsoft 365 applications, are powered by Windows Copilot Runtime. It includes the Windows Copilot Runtime APIs, powered by over 40 on-device AI models and AI frameworks to bring your own AI models to Windows, offering a secure, efficient and reliable platform for developers to create innovative experiences. Today, we're announcing new imaging AI APIs in Windows Copilot Runtime, like those used by Click to Do and our Microsoft 365 experiences, so your developers can use them to enhance your commercial or line of business applications.

(Onscreen text: aka.ms/WindowsCopilotRuntime)

For example, LiquidText, a note-taking app that offers a fast, natural way to review, gather and organize information across all your documents. Now, on Copilot+ PC, we're launching an experience called auto-citation. This lets you easily add citations to your notes and is powered by natural language search. This is a great example of an ISV bringing their own AI models and scaling across Windows using our AI frameworks to create new value with an experience that is reliable, fast, secure and private. Whether you're one of the world's largest ISVs like our very own M365, or a small company just getting started, join the hundreds of apps already developing with Windows Copilot Runtime. Learn more about how you can get started at the Windows Copilot Runtime breakout session tomorrow morning at 9:45. This is just the start. The future of business AI on Windows is here, and we cannot wait to see what you do with the power and possibilities of Copilot+ PCs. Thank you.

[APPLAUSE]

Dave Dame: What I want to do near this end of my career is to make sure there are going to be many others after me and along me that get to get the life that I've had. I'm Dave Dame, Senior Director of Product Accessibility at Microsoft. At Microsoft, we want to empower everyone on the planet to achieve more. Voice access, wake up. It would usually take me 14 minutes to do an email. Draft an email about the annual fundraising campaign. Now with Windows and M365 Copilot, I can generate it in minutes. New paragraph, thanks, comma. New line, Dave. It makes it possible for people with disabilities, but it gives everyone else options and freedoms because we're using the natural things we do as humans to be more productive and be more efficient, which then results into getting the most out of the collective. You're getting that time, that precious time, to think, to create, to design, to be able to reinvent something new instead of just iterating on what has been. When you design for accessibility, it is innovation. Design for one and extend to many.

[APPLAUSE]

Pavan Davaluri: Just think about the diversity of lives and businesses Windows touches. With this kind of impact comes incredible opportunity and responsibility. We believe that AI has the power to make technology more accessible and more inclusive, so we're designing Windows to be accessible for all. Let's bring this together. You told us security is your top priority, so we shared how we're working to make Windows the most secure and most reliable platform for the future and now with the Windows Resiliency Initiative. You asked us for help to modernize your endpoints, so we're working hard to make it easier than ever to move to Windows 11 for your fleet across cloud and client. Finally, you asked how you can bring AI capabilities for your employees, so with the power of Microsoft 365 Copilot,

Windows and Copilot+ PCs, we showed you the journey we're on. This is just the start of a new AI era at work. There is so much more to come. We invite you to hear more from our breakout sessions. Thank you all for being here. You inspire us, you push us to innovate and to deliver for both today's and tomorrow's business needs. I'm grateful to be on this journey with you. Thank you.

[APPLAUSE]

END